Authentify, Inc.
8745 West Higgins Road, Suite 240
Chicago, Illinois 60631
www.authentify.com
773-243-0300

September 8, 2006

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW . Room TW-A325
Washington, D.C. 20554

Dear Ms. Dortch,

This letter is to provide notice that on September 7, 2006, Peter Tapling and James Woodhill of Authentify, Inc. and Stan Szwalbenest of JPMorganChase met with Carol Simpson, Nick Alexander, Ann Stevens and Mary McManus of the Wireline Enforcement Bureau regarding IP Enabled Services WC Docket No. 04-36.

Our purpose was to urge the FCC to consider the commercial value of trust in the Public Switched Telephone Network when determining an appropriate level of regulation for IP enabled services. Specifically, parties which rely on telephone numbers for authentication and authorization purposes should be able to determine who owns a telephone number and how a given telephone number is being routed for any given call, among other considerations.

This letter submitted electronically via the FCC Electronic Comment File Submission web page at http://gullfoss2.fcc.gov/prod/ecfs/upload_v2.cgi.

Sincerely,

/s/ Peter Tapling
President & CEO
Authentify, Inc.

Attachment

Fraud and the Telephone Network

A Briefing for the Federal Communications Commission

September 7, 2006

Peter Tapling
President & CEO
Authentify, Inc.
peter.tapling@authentify.com
773-243-0322

Purpose

- Commerce relies on trust in the PSTN
- Discuss VoIP market structure and specific risk challenges
- Discuss other risk issues of note
- Explore ways industry and FCC can work together to mitigate commerce risk
  - Do we want to protect the PSTN as national infrastructure?

Commerce Requires Trusted Communication

- Public Switched Telephone Network provided a trusted platform for communication
  - Difficult to breach
  - Legal implications for misuse
  - Control/reporting/auditing
- Telephone numbers represent an “address” of sorts
  - Historically could map to geography
- “Virtual” commerce has relied on PSTN

PSTN as a Risk Management Tool

- When a transaction is at risk, first line of defense is to call the customer!
- Phone numbers represent a fixed “real estate”, each number is “owned” by someone.
- Reverse lookup information for land lines
  - Would be very helpful for cell phones
- Phone number as geography/address proxy
  - How ANI is used today when registering a credit card
- LIDB/LERG/LNP as resource
  - Provisioning information
    - Land line/cell phone? Payphone? Commercial/Consumer?
  - Length of billing relationship in good standing?
  - Has a number been ported?
- SS7 – real time info
  - Destination line currently being forwarded?

AUTHENTIFY

Threats to Trust in the PSTN

- ANI spoofing
- VoIP
- Other Internet controlled services
  - Voice mail, call forward, etc.
  - Relay calling

AUTHENTIFY

Voice Over Internet Protocol – VoIP

- What's different?
  - Allows access to the previously protected telephone number space without the previously required reporting
- Why is it a problem?
  - Parties wishing to hide their true identity/location/purpose can benefit from the trust in the PSTN without having to follow its rules
- Risk accelerating as VoIP services make up a greater percentage of telephone lines

VoIP – Market Structure

- VoIP used in many different contexts
  - Important risk factors include
    - who owns/controls/accesses network?
    - Does call “touch” PSTN?
- Risk depends on structure of VoIP usage

Computer to Computer

- No risk to PSTN trust
  - Does not claim to be part of PSTN
  - Network can be private or public

Carrier Backbone

- No risk to trust in PSTN
  - Is part of PSTN, controlled by carriers
  - Network is private, highly secure

Commercial Services

- Limited risk to trust in PSTN
  - Part of PSTN for DID, ANI purposes
  - Network can be private or public, but typically maintained securely
  - Services contracted with reporting carrier (CPNI captured)

Retail VoIP

- High to extreme risk to trust in PSTN
  - Part of PSTN for DID, ANI purposes
  - Semi-private to public network
    - “Static” (Comcast) vs. “Dynamic” (Vonage)
  - No central security over network
  - Services *not* contracted with reporting carrier

VoIP Risks Not Considered

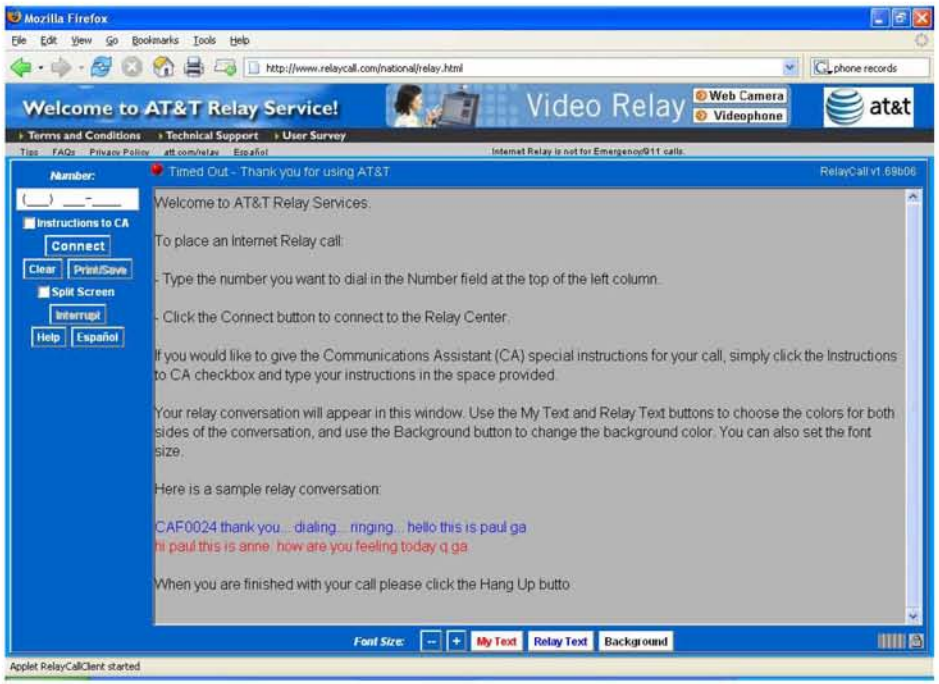
- Endpoint authentication
- Packet protection “over the wire”
- Service theft
- Denial of service
- Availability/reliability

AUTHENTIFY

Internet Controlled Services

- Controlled by username/password via Internet
  - Subjects PSTN to Internet attacks such as phishing and keyboard loggers
- Examples
  - Unified Messaging services
    - Call forwarding, voice mail, fax forwarding
  - Remote Call Forward services

Relay Calling



- Allows for a fully anonymous use of the PSTN
- Use by thieves increasing rapidly

Suggestions

- Encourage stronger authentication for Internet controlled services
- Require greater disclosure for use of Relay Services
- Must treat VoIP services as telephone service
  - Establish a provisioning type flag for VoIP and require registration when telephone number is “sold”
    - Hold each phone number registration to the same standard
  - Capture/allow access to CPNI for VoIP lines
  - Provide for real-time access to SIP gateway routing information by telephone number or call
  - CALEA and e911 would benefit as well

Discussion

- Thank you for your time and attention
- What can “industry” do to help?
- Next steps…